tenable network security

Verificações de Credenciais do Nessus para Unix e Windows

17 de janeiro de 2014

(Revisão 32)

Sumário

Introdução

Este artigo descreve como executar varreduras de rede autenticadas com o scanner de vulnerabilidades **Nessus** da Tenable Network Security. As varreduras de rede autenticadas permitem que uma auditoria remota de rede obtenha dados no host, como patches ausentes e configurações do sistema operacional. Envie seus comentários e sugestões para o e-mail support@tenable.com.

O Nessus usa a funcionalidade de login remoto em hosts Unix por meio do Secure Shell (SSH). Nos hosts Windows, o Nessus usa diversas tecnologias de autenticação da Microsoft.

Observe que o Nessus também usa o Protocolo Simples de Gerenciamento de Rede (SNMP) para fazer consultas de versão e informações a roteadores e switches. Embora esta seja uma forma de "verificação local", não é descrita neste documento.

Este documento também faz diversas referências ao "Nessus", mas os conceitos básicos também são válidos para o SecurityCenter da Tenable.

Padrões e convenções

Em toda a documentação, os nomes de arquivos, daemons e executáveis são indicados com a fonte **`courier bold`**, como **`gunzip`**, **`httpd`** e **`/etc/passwd`**.

As opções de linhas de comando e palavras-chave também são indicadas com a fonte **`courier bold`**. O exemplos de linhas de comando podem ou não conter o prompt da linha de comando e o texto gerado pelos resultados do comando. Os exemplos de linhas de comando exibirão o comando executado em **`courier bold`** para indicar o que o usuário digitou, enquanto que o exemplo de saída gerado pelo sistema será indicado em `courier` (sem negrito). Um exemplo da execução do comando **`pwd`** do Unix é apresentado a seguir:

```
# pwd
/home/test/
#
```

As observações e considerações importantes são destacadas com este símbolo nas caixas de texto escurecidas.

As dicas, exemplos e práticas recomendadas são destacados com este símbolo em branco sobre fundo azul.

Visão geral das Verificações de Credenciais do Nessus

O scanner Nessus da Tenable é um scanner de vulnerabilidades de rede muito eficaz, com um banco de dados abrangente de plugins que verificam diversos tipos de vulnerabilidades que podem ser exploradas remotamente. Além da varredura remota, o scanner Nessus também pode ser usado para examinar para exposições locais.

Objetivo

A varredura externa de vulnerabilidades de rede permite obter uma "visualização instantânea" dos serviços de rede oferecidos e das vulnerabilidades que podem conter. No entanto, é apenas uma perspectiva externa. É importante saber quais serviços locais estão sendo executados e identificar as exposições de segurança contra ataques locais ou parâmetros de configuração que possam expor o sistema a ataques externos e que não podem ser detectados através de uma varredura externa.

Em uma avaliação típica de vulnerabilidades de rede, uma varredura remota é executada nos pontos de presença externos e uma varredura local é realizada dentro da rede. Nenhuma dessas varreduras é capaz de determinar as exposições locais no sistema-alvo. Algumas das informações obtidas dependem das informações exibidas, que podem ser inconclusivas ou incorretas. Por meio de credenciais seguras, o scanner Nessus pode receber acesso local para

verificação do sistema-alvo sem a necessidade de um agente. Isto pode facilitar a verificação de uma rede muito extensa e determinar as exposições locais ou violações de conformidade.

O problema de segurança mais comum em uma organização é que os patches de segurança não são aplicados em tempo hábil. A varredura credenciada do Nessus pode determinar rapidamente quais sistemas possuem correções desatualizadas. Isto é importante nos casos em uma nova vulnerabilidade é anunciada e a administração executiva requer uma resposta rápida sobre o impacto na organização.

Outra grande preocupação das organizações é determinar o cumprimento de políticas internas, normas do setor (como os referenciais CIS (Center for Internet Security) ou legislações (Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA) ou HIPAA). As organizações que aceitam cartões de crédito devem comprovar o cumprimento das normas PCI DSS (Padrões de Segurança de Dados da Indústria de Cartões de Pagamento). Existem muitos casos divulgados em que as informações de cartões de crédito de milhões de clientes foram expostas. Isto representa prejuízos financeiros consideráveis para os bancos responsáveis pela cobertura dos pagamentos e multas pesadas ou a perda dos direitos de aceitação de cartões de crédito por parte dos comerciantes das administradoras que sofreram a violação.

Nível de acesso

As varreduras credenciadas podem executar as mesmas operações que um usuário local. O nível de varredura depende dos privilégios concedidos à conta de usuário que o Nessus está configurado para usar.

Os usuários sem privilégios com acesso local a sistemas Unix podem determinar problemas básicos de segurança, como níveis de patch ou itens no arquivo **`/etc/passwd`**. Para informações mais abrangentes, como dados de configuração do sistema ou permissões de arquivos em todo o sistema, é necessária uma conta com privilégios “raiz”.

As varreduras credenciadas em sistemas Windows exigem o uso de uma conta com nível de administrador. Vários boletins e atualizações de software da Microsoft podem prejudicar a confiabilidade da leitura do registro para determinar o nível de patch de software sem privilégios de administrador. O acesso administrativo é necessário para executar a leitura direta do sistema de arquivos. Isto permite que o Nessus se conecte a um computador e realize a análise direta de arquivos para determinar o verdadeiro nível de patch dos sistemas que estão sendo avaliados. No Windows XP Pro, o acesso aos arquivos funciona apenas com uma conta de administrador local se a política “Acesso à rede: Modelo de compartilhamento e segurança de contas locais” for alterada para “Clássico – os usuários locais são autenticados como eles próprios”.

Uma auditoria, para conformidade com SCAP, requer o envio de um executável para o host remoto. Em sistemas com software de segurança (por exemplo: McAfee Host Intrusion Prevention), ele poderá bloquear ou colocar em quarentena o executável necessário para a auditoria. Nesses sistemas, uma exceção deve ser criada para o host ou para o executável enviado.

Tecnologias usadas

O desafio de realizar uma varredura credenciada é fornecer credenciais privilegiadas para o scanner de maneira segura e automática. O objetivo de verificação das exposições de segurança seria anulado se o processo criasse uma exposição ainda maior. O Nessus permite o uso de vários métodos seguros para solucionar o problema nas plataformas Unix e Windows.

Sistemas Unix

Em sistemas Unix, o Nessus usa programas com base no protocolo Secure Shell (SSH) versão 2 (por exemplo: OpenSSH, Solaris SSH, etc.) para verificações realizadas no host. Esse mecanismo criptografa os dados em trânsito para protegê-los contra visualização por programas sniffer. O Nessus reconhece três tipos de métodos de autenticação para uso com o SSH: Nome de usuário e senha, chaves públicas/privadas e Kerberos.

Nome de usuário e senha

Embora seja compatível, a Tenable não recomenda o uso da combinação de nome de usuário e senha para autenticação com SSH. As senhas estáticas estão sujeitas a ataques de “intermediários” e de força bruta se forem usadas por muito tempo.

Chaves públicas/privadas

A criptografia de chave pública, também conhecida como criptografia de chave assimétrica, é um mecanismo de autenticação mais seguro, pois usa um par de chaves públicas e privadas. Na criptografia assimétrica, a chave pública é usada para criptografar os dados e a chave privada é usada para decodificá-la. O uso de chaves públicas e privadas é

um método mais seguro e flexível de autenticação com SSH. O Nessus oferece suporte para os formatos de chaves DSA e RSA.

Kerberos
O Kerberos, desenvolvido pelo Projeto Athena do MIT, é uma aplicação cliente/servidor que usa um protocolo de criptografia simétrica de chaves. Na criptografia simétrica, a chave usada para criptografar os dados é a mesma usada para decodificá-los. As organizações instalam um KDC (Centro de Distribuição de Chaves) que contém todos os usuários e serviços que exigem a autenticação Kerberos. Os usuários se autenticam no Kerberos ao solicitar um TGT (Ticket Granting Ticket). Depois de ser concedido ao usuário, o TGT poderá ser usado para solicitar tickets de serviço do KDC outros serviços do Kerberos. O Kerberos usa o protocolo de criptografia DES CBC (Cipher Block Chain) para criptografar todas as comunicações.

A implementação da autenticação do Kerberos pelo Nessus para SSH reconhece os algoritmos de criptografia "aes-cbc" e "aes-ctr". Um resumo de como o Nessus interage com o Kerberos é mostrado a seguir:

- O usuário final envia o IP do KDC
- **`nessusd`** pergunta ao **`sshd`** se reconhece a autenticação do Kerberos
- **`sshd`** responde afirmativamente
- **`nessusd`** solicita um TGT do Kerberos junto com o login e a senha
- O Kerberos encaminha um ticket ao **`nessusd`**
- **`nessusd`** envia o ticket ao **`sshd`**
- **`nessusd`** é conectado

Sistemas Windows
O Nessus permite o uso de vários tipos diferentes de métodos de autenticação para sistemas Windows. Cada um dos métodos requer um nome de usuário, uma senha e um nome de domínio (opcional para a autenticação).

LANMAN
O método de autenticação Lanman era predominante no Windows NT e nas primeiras versões do Windows 2000 Server. O método não é usado nas versões mais recentes do Windows, mas é mantido por motivo de compatibilidade com as versões anteriores.

NTLM e NTLMv2
O método de autenticação NTLM, que acompanha o Windows NT, é mais seguro que a autenticação com o método LanMan. No entanto, a versão aprimorada, NTLMv2, apresenta recursos de criptografia mais seguros que o NTLM, pois é o método de autenticação padrão escolhido pelo Nessus ao efetuar o login em um servidor Windows.

Assinatura SMB
A assinatura SMB é uma soma de verificação criptográfica aplicada a todo o tráfego de SMB de/para um servidor Windows. Vários administradores de sistemas ativam este recurso nos servidores para garantir que os usuários remotos sejam 100% autenticado e façam parte de um domínio. O recurso é usado automaticamente pelo Nessus se for exigido pelo servidor Windows remoto.

SPNEGO
O protocolo SPNEGO (Simple and Protected Negotiate) oferece o recurso de acesso unificado (SSO) de um cliente Windows para vários recursos protegidos, por meio de credenciais de login dos usuários do Windows. O Nessus oferece suporte para SPNEGO com o NTLMSSP com autenticação LMv2 ou Kerberos com encriptação RC4.

Kerberos
O Nessus também permite a autenticação pelo Kerberos em um domínio do Windows. Para configurá-lo, o endereço IP do controlador de domínio do Kerberos (endereço IP do servidor Windows Active Directory) deve ser fornecido.

NTLMSSP (NT Lan Manager Security Support Provider) e LMv2
Se um esquema de segurança estendido (como o Kerberos ou o SPNEGO) não for reconhecido ou falhar, o Nessus tentará fazer o login por meio da autenticação NTLMSSP/LMv2. Se isso falhar, o Nessus tentará fazer o login usando a autenticação NTLM.

Nomes de usuário, senhas e domínios do Windows
O campo de domínio do SMB é opcional e o Nessus poderá fazer logon com as credenciais de domínio sem o campo. O nome de usuário, senha e domínio opcional referem-se a uma conta reconhecida pelo computador de destino. Por exemplo: se o nome de usuário for “joesmith” e a senha “`my4x4mpl3`”, o servidor Windows tentará localizar primeiro o nome de usuário na lista local de usuários do sistema e determinará se faz parte de um domínio.

O nome real do domínio só será necessário se o nome da conta no domínio for diferente do nome da conta no computador. É perfeitamente possível ter uma conta “Administrador” em um servidor Windows e no domínio. Neste caso, para fazer logon no servidor local, o nome de usuário “Administrador” será usado com a senha desta conta. Para fazer logon no domínio, o nome de usuário “Administrador” também deve ser usado, mas com a senha e o nome do domínio.

Independentemente das credenciais usadas, o Nessus sempre tenta fazer login em um servidor Windows com as seguintes combinações:

- “Administrador” sem senha
- Nome de usuário e senha aleatórios para verificação de contas de visitantes
- Nenhum nome de usuário ou senha para testar sessões nulas

Verificações de credenciais em plataformas baseadas em Unix

O processo descrito nesta seção permite que executar verificações de segurança locais em sistemas Unix (por exemplo: Linux, Solaris, Mac OS X). O daemon DE SSH usado neste exemplo é O OpenSSH. Se houver uma variante comercial do SSH, o procedimento pode ser um pouco diferente.

Para permitir verificações de segurança locais, podem ser usados dois métodos básicos:

1. Uso de um par de chaves SSH privadas/públicas
2. Credenciais do usuário e acesso ao **`sudo`** ou credenciais de acesso ao **`su`**

Pré-requisitos

Requisitos de configuração do SSH

O Nessus 5 oferece suporte para os algoritmos blowfish-CBC, AESXXX-CBC (AES128, AES192 e AES256), 3DES-CBC e AES-CTR.

Algumas variantes comerciais do SSH não reconhecem o algoritmo blowfish, possivelmente por motivos de exportação. Também é possível configurar um servidor SSH para aceitar apenas certos tipos de criptografia. Verifique o servidor de SSH para saber se o algoritmo correto é reconhecido.

Privilégios do usuário

Para maior eficácia, o usuário do SSH deve ser capaz de executar qualquer comando no sistema. Em sistemas Unix, isto é conhecido como privilégios “**`root`**”. Embora seja possível executar algumas verificações (como níveis de patch) por meio de acesso sem privilégios, as verificações completas de conformidade que auditam a configuração do sistema e as permissões de arquivo requerem o acesso “root”. Por isso, é recomendável, sempre que possível, usar chaves de SSH em vez de credenciais.

Requisitos de configuração do Kerberos

Se o Kerberos for usado, **`sshd`** deve ser configurado com suporte para o Kerberos para confirmar o ticket do KDC. As consultas inversas ao DNS devem ser configuradas corretamente para que isto funcione. O método de interação do Kerberos deve ser **`gssapi-with-mic`**.

Permitir verificações de segurança locais de SSH no Unix

Esta seção apresenta o procedimento geral para ativação do SSH entre os sistemas envolvidos nas verificações de credenciais pelo Nessus. A seção não deve ser considerada um tutorial abrangente do SSH. O leitor deve ter conhecimento necessário dos comandos do sistema Unix.

Geração de chaves SSH públicas e privadas

O primeiro passo é gerar um par de chaves privadas/públicas para uso pelo scanner Nessus. As chaves podem ser geradas por qualquer sistema Unix por meio de qualquer conta de usuário. No entanto, é importante que as chaves sejam de propriedade do usuário Nessus definido.

Para gerar o par de chaves, use **`ssh-keygen`** e salve-o em um local seguro. No exemplo a seguir, as chaves são geradas em uma instalação do Red Hat ES 3.

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
       /home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Não transferir a chave privada para nenhum outro sistema que não seja o sistema executado no servidor Nessus. Quando **`ssh-keygen`** solicitar uma frase-senha, digite uma frase-senha forte ou pressione “Return” (Voltar) duas vezes (ou seja, não define nenhuma frase-senha). Se uma frase-senha for especificada, use as opções Policies (Políticas) -> Credentials (Credenciais)-> SSH settings (Configurações SSH) para que o Nessus use a autenticação por chaves.

Os usuários do Nessus no Windows podem copiar ambas as chaves no diretório principal do aplicativo Nessus no sistema que executa o Nessus (**`C:\Program Files\Tenable\Nessus`** é o diretório predefinido) e, em seguida, copiar a chave pública nos sistemas de destino, se necessário. Isto facilita o gerenciamento dos arquivos das chaves pública e privada.

Como criar contas de usuário e chaves SSH

Em cada sistema de destino a ser examinado por meio de verificações de segurança locais, crie uma nova conta de usuário dedicada ao Nessus. Esta conta de usuário deve ter exatamente o mesmo nome em todos os sistemas. Neste documento, chamaremos o usuário de “nessus”, mas pode-se usar qualquer nome.

Depois que a conta for criada para o usuário, verifique se a conta não tem nenhuma senha válida definida. Nos sistemas Linux, as novas contas de usuário são normalmente bloqueadas, a menos que uma senha inicial seja definida. Se for usada uma conta para a qual uma senha tenha sido definida, use o comando “**`passwd –l`**” para bloquear a conta.

É preciso criar o diretório no diretório inicial dessa nova conta para manter a chave pública. Neste exercício, o diretório será **`/home/nessus/.ssh`**. Um exemplo para os sistemas Linux é apresentado abaixo:

```
# passwd –l nessus
# cd /home/nessus
# mkdir .ssh
#
```

Nos sistemas Solaris 10, a Sun aprimorou o comando “**`passwd(1)`**” para distinguir entre contas bloqueadas e sem login. Isto garante que uma conta de usuário bloqueada não possa ser usada para executar comandos (por exemplo: tarefas

cron). As contas sem login são usadas apenas para executar comandos e não funcionam em uma sessão de login interativo. As contas levam o token "NP" no campo de senha de **/etc/shadow**. Para configurar uma conta sem login e criar o diretório da chave pública de SSH no Solaris 10, execute os seguintes comandos:

```
# passwd -N nessus

# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

Depois de criar a conta de usuário, é preciso transferir a chave para o sistema ao colocá-la no diretório adequado e definir as permissões corretas.

Exemplo

Para o sistema que contém as chaves, copie de forma segura a chave pública no sistema a ser examinado, conforme indicado abaixo. 192.1.1.44 é um exemplo de sistema remoto que será testado com as verificações de host.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

É possível também copiar o arquivo do sistema em que o Nessus está instalado com o comando de FTP "**sftp**" seguro. Observe que o arquivo no sistema de destino deve ter o nome "authorized_keys".

Retorne ao sistema que hospeda a chave pública

Defina as permissões no diretório **/home/nessus/.ssh** e no arquivo **authorized_keys**.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Repita esse processo em todos os sistemas que passarão por testes de SSH (começando em "Como Criar uma Conta de Usuário e Criar a Chave SSH" acima).

Teste para verificar se as contas e as redes estão configuradas corretamente. Com o comando "**id**" simples do Unix no scanner Nessus, execute o comando a seguir:

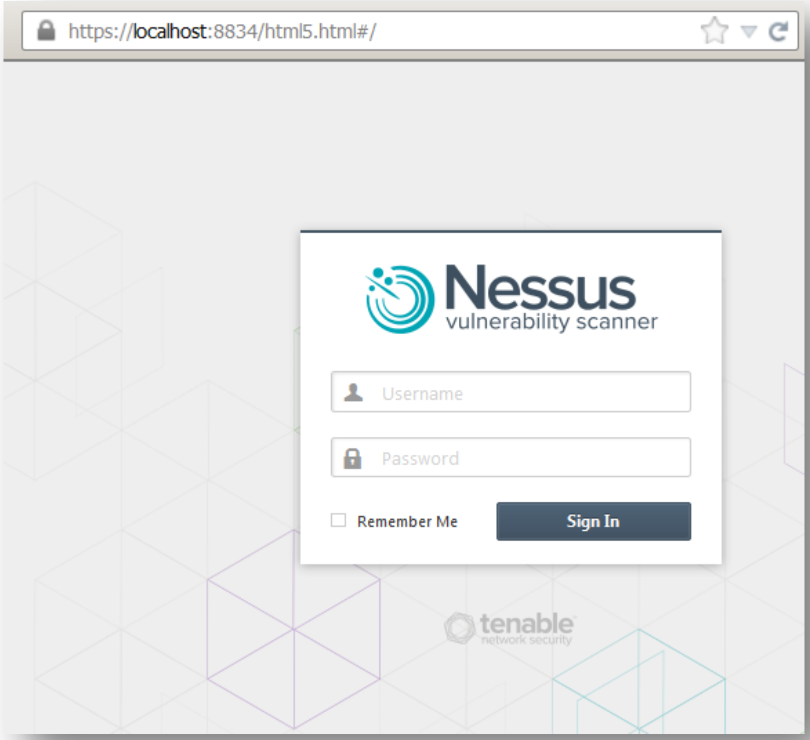
```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

Se o comando gerar informações sobre o usuário nessus, a troca de chaves será bem-sucedida.

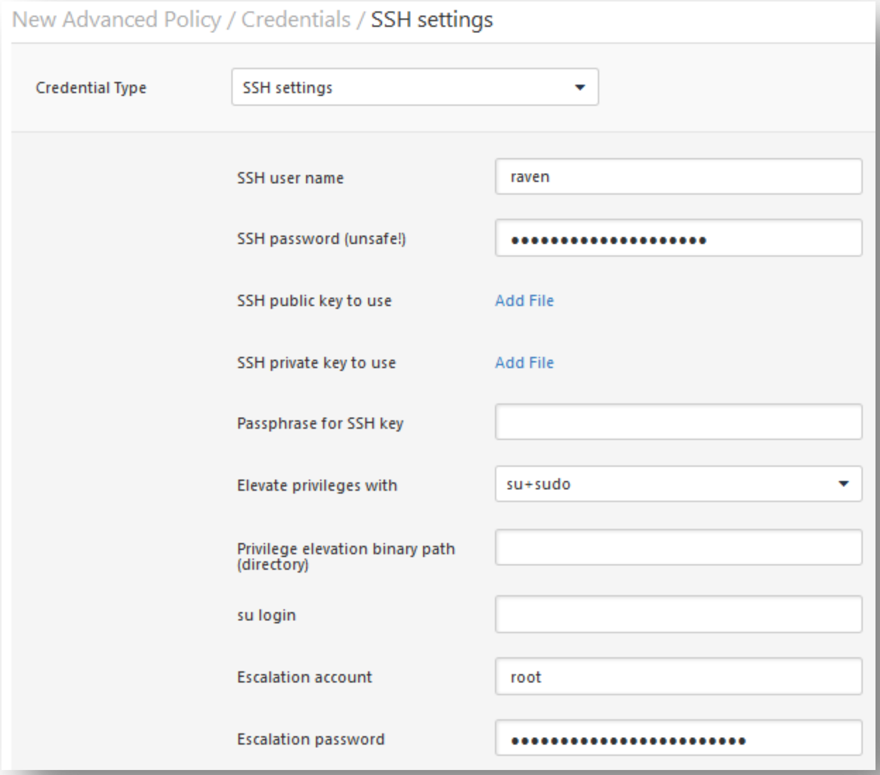
Configuração do Nessus para verificações de SSH no host

Interface de usuário do Nessus

Caso ainda não tenha sido feito, copie de maneira segura os arquivos das chaves pública e privada no sistema usadas para acessar o scanner Nessus.



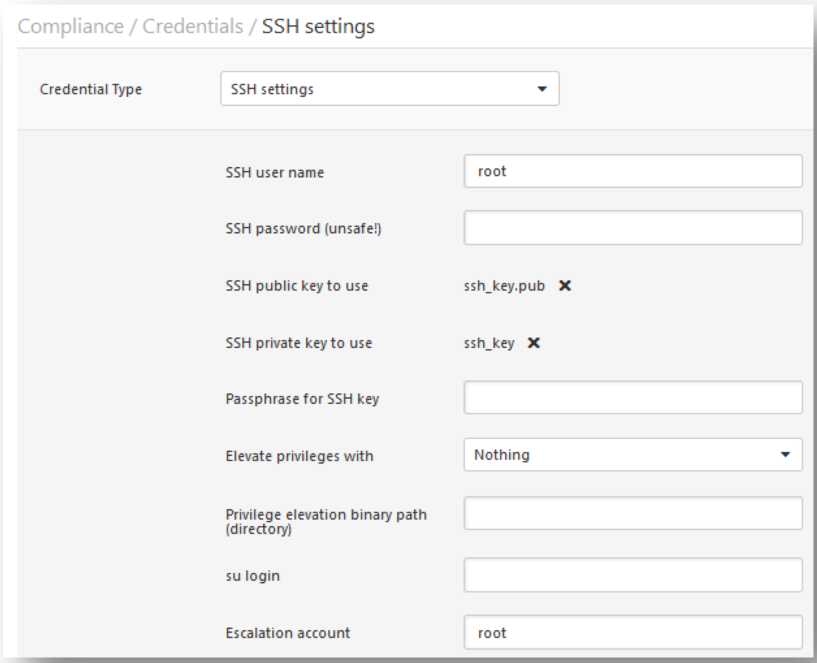
Abra um navegador e conecte-se à interface de usuário do scanner Nessus como no exemplo acima e clique na guia “Policies” (Políticas). Crie uma nova política ou edite uma política existente e selecione a guia "Credentials" (Credenciais) à esquerda. Selecione “SSH settings” (Configurações SSH) no menu suspenso na parte superior, conforme mostrado abaixo:



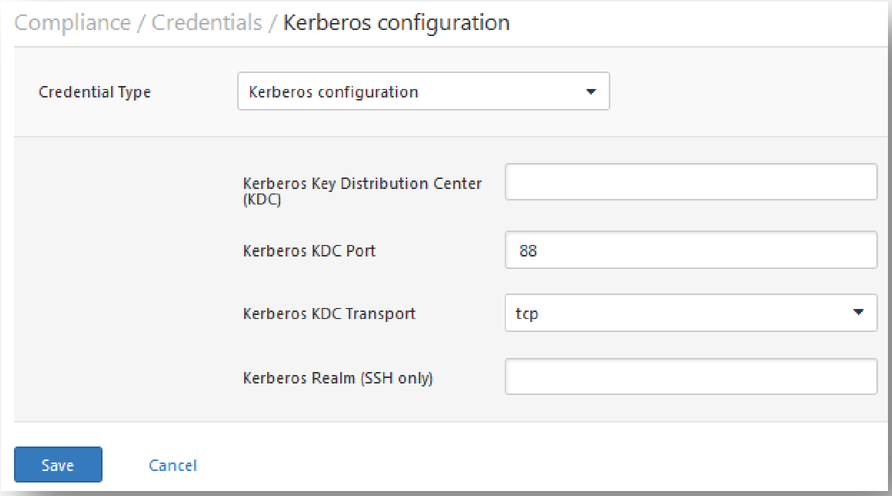
- No item “SSH user name” (Nome de usuário SSH), digite o nome da conta dedicada ao Nessus em cada um dos sistemas submetidos à varredura. O padrão é “root”.
- Se a senha SSH for usada, digite-a no campo “SSH password” (Senha SSH).
- Se as chaves SSH forem usadas em vez de uma senha (recomendado), clique no botão “Select” (Selecionar) ao lado do campo identificado como “SSH public key to use” (Chave SSH pública a ser usada) e localize o arquivo de chave pública no sistema local.
- No item “SSH private key to use” (Chave SSH privada a ser usada), clique no botão “Select” (Selecionar) e localize o arquivo de chave privada associada à chave pública acima no sistema local.
- Se a senha da chave SSH for usada (opcional), digite-a no campo “Passphrase for SSH key” (Frase-senha da chave SSH).
- Os usuários do Nessus e do SecurityCenter também podem usar os comandos “**su**” ou “**sudo**” no campo “Elevate privileges with” (Elevar privilégios com) e uma senha diferente.
- Se um arquivo **known_hosts** do SSH estiver disponível juntamente com a política de varredura no campo no “SSH known_hosts file” (Arquivo known_hosts do SSH), o Nessus tentará fazer o login nos hosts nesse arquivo somente. Isto garante que o mesmo nome de usuário e a mesma senha usados para auditar os servidores SSH conhecidos não sejam usados para tentativas de login em sistemas fora de seu controle.

As varreduras credenciadas mais eficazes são aquelas em que as credenciais fornecidas têm privilégios “root”. Uma vez que muitos locais não permitem o login remoto como root, os usuários do Nessus podem acessar “**su**” ou “**sudo**” com uma senha distinta em uma conta criada para ter os privilégios “**su**” ou “**sudo**”.

Veja a seguir um exemplo de imagem de tela “**sudo**” juntamente com chaves SSH. Neste exemplo, a conta de usuário é “audit”, que foi adicionada ao arquivo **/etc/sudoers** no sistema a ser verificado. A senha fornecida é a senha para a conta “audit” e não a senha raiz. As chaves SSH correspondem às chaves geradas para a conta “audit”:



Se o Kerberos for usado, um scanner Nessus deve ser configurado para autenticação do KDC. Selecione “Kerberos configuration” (Configuração do Kerberos) no menu suspenso, conforme indicado abaixo:



A porta padrão do KDC é “88” e o protocolo de transporte padrão é “udp”. O outro valor para o transporte é “tcp”. O nome do nome do Kerberos Realm e o endereço IP do KDC são obrigatórios.

> Observe que o usuário já deve ter um ambiente Kerberos estabelecido para usar este método de autenticação.

Neste ponto, clique em “**Submit**” (Enviar) na parte inferior da janela para concluir a configuração. A nova política de varredura será adicionada à lista de políticas de varredura gerenciadas.

Linha de comando do Nessus para Unix

O Nessus permite verificações no host a partir da versão 2.2.0 e exige que o suporte SSL esteja incorporado. Execute o comando “**`nessusd -d`**” para verificar se a versão e as bibliotecas SSL corretas estão instaladas, da seguinte maneira:

```
# nessusd -d
[root@squirrel sbin]# ./nessusd -d
This is Nessus 5.0.1. [build R23100] for Linux 2.6.18-53.1.6.el5
compiled with gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)
Current setup :
        flavor                         : es5-x86
        nasl                           : 5.0.1
        libnessus                      : 5.0.1
        SSL support                    : enabled
        SSL is used for client / server communication
        Running as euid                : 0
Magic hash: 49edd1433ffad7b87b446a4201faeedf  -
OpenSSL: OpenSSL 1.0.0g 18 Jan 2012
```

Uso dos arquivos .nessus

O Nessus pode salvar políticas de varredura configuradas, alvos de rede e relatórios como arquivo **`.nessus`**. A seção acima “Interface de usuário do Nessus” descreve a criação de um arquivo **`.nessus`** que contém credenciais de SSH. Para obter instruções sobre como executar uma varredura por linha de comando com o arquivo **`.nessus`**, consulte o “Nessus User Guide” (Guia do usuário do Nessus) disponível em:

http://www.tenable.com/products/nessus/documentation

Uso dos arquivos .nessusrc

Se os arquivos “**`.nessusrc`**” forem criados manualmente, existem vários parâmetros que podem ser configurados para especificar a autenticação SSH. Um exemplo de listagem vazia é apresentado a seguir:

```
Use SSH to perform local security checks[entry]:SSH user name : =
Use SSH to perform local security checks[file]:SSH public key to use : =
Use SSH to perform local security checks[file]:SSH private key to use : =
Use SSH to perform local security checks[password]:Passphrase for SSH key : =
SSH settings[entry]:SSH user name : =
SSH settings[password]:SSH password (unsafe!) : =
SSH settings[file]:SSH public key to use : = no
SSH settings[file]:SSH private key to use : =
SSH settings[password]:Passphrase for SSH key : =
```

Se o Kerberos for usado, configure um scanner Nessus para se autenticar a um KDC ao digitar as seguintes informações no arquivo **`nessusrc`** do scanner:

```
Kerberos KDC port : 88
Kerberos KDC Transport : udp
Kerberos Realm (SSH Only) : myrealm
```

```
Kerberos Key Distribution Center (KDC): 192.168.20.66
```

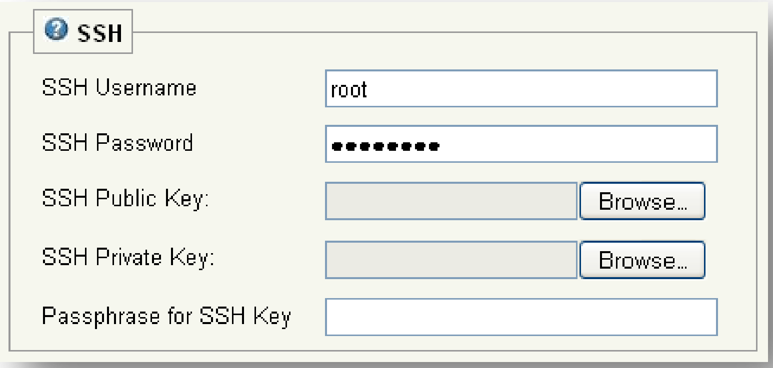
A porta padrão do KDC é “88” e o protocolo de transporte padrão é “udp”. O outro valor para o transporte é “tcp”. O nome do nome do Kerberos Realm e o endereço IP do KDC são obrigatórios.

> Observe que o usuário já deve ter um ambiente Kerberos estabelecido para usar este método de autenticação.

Como usar credenciais SSH com o Tenable SecurityCenter

Para usar as credenciais SSH com o SecurityCenter, envie as chaves SSH pública e privada geradas para o console do SecurityCenter. Não as instale diretamente nos scanners Nessus, pois o SecurityCenter baixa essas credenciais para o scanner Nessus quando a varredura for iniciada.

Veja a seguir um exemplo de uma parte da tela “Edit Scan Options” (Editar opções de varredura) ao editar as opções de uma política. Os três últimos campos são usados para especificar uma conta e as chaves SSH pública e privada específicas que serão usadas no teste. A chave SSH pública deve ser colocada em cada host Unix a ser testado com as “verificações locais”.



O SecurityCenter é distribuído com várias políticas de vulnerabilidade predefinidas, nas quais todas as “verificações locais” estão ativadas para cada sistema operacional. No entanto, as políticas devem ser copiadas e duas chaves SSH públicas/privadas e uma conta de usuário específicos devem ser acrescentados para que possam ser usadas de maneira operacional.

Os pares de chaves SSH pública/privada são gerenciados pelo SecurityCenter e serão transmitidos a cada scanner Nessus gerenciado.

> Quando as chaves públicas de SSH estiverem instaladas nos hosts Unix desejados e as chaves privadas instaladas no SecurityCenter, uma relação de confiança será estabelecida e um usuário poderá fazer login em cada host Unix a partir dos scanners Nessus. Se a segurança dos scanners Nessus for comprometida, será necessário gerar novos pares de chaves SSH públicas/privadas..

Verificações de credenciais em plataformas Windows

Pré-requisitos

Privilégios do usuário

Um erro muito comum consiste em criar uma conta local sem privilégios suficientes para fazer logon de maneira remota ou para executar alguma ação. Normalmente, o Windows atribui às novas contas locais os privilégios de “Guest” (Visitante) caso façam logon remoto. Isto impede que as auditorias remotas de vulnerabilidades sejam realizadas. Outro erro comum é aumentar o nível de acesso dos usuários “Guest”. Isto enfraquece a segurança do seu servidor Windows.

Permitir logins do Windows para auditorias locais e remotas

O aspecto mais importante das credenciais do Windows é que a conta usada para executar as verificações devem ter privilégios para acessar todos os arquivos e entradas de registro necessários e em muitos casos, isso significa ter privilégios administrativos. Se o Nessus não receber as credenciais de uma conta administrativa, poderá, na melhor das hipóteses, ser usado para executar verificações de patches no registro. Embora seja um método válido para determinar se um patch foi instalado, é incompatível com algumas ferramentas de gerenciamento de patches de terceiros, que podem deixar de definir a chave na política. Se o Nessus tiver privilégios administrativos, verificará a versão da biblioteca de vínculos dinâmicos (**`.dll`**) no computador remoto, o que é extremamente mais preciso.

Configurando uma conta local

Para configurar um servidor Windows fora de um domínio com credenciais a serem usadas, basta criar uma conta exclusiva como administrador.

Verifique se a conta não está configurada com o padrão normal “Somente convidados: usuários locais autenticados como convidados”. Alterne para o modo “Clássico: os usuários locais são autenticados como eles próprios”.

Para configurar o servidor para permitir logins de uma conta de domínio, o modelo de segurança “Clássico” deve ser usado. Para isso, execute as etapas a seguir:

1. Abra “Política de Grupo” e clique em “Iniciar”, “Executar”, digite “**`gpedit.msc`**” e clique em “OK”.

2. Selecione Configuração do Computador -> Configurações do Windows -> Configurações de segurança -> Políticas Locais -> Opções de segurança.

3. Na lista de políticas, clique em “Acesso à rede: modelo de compartilhamento e segurança para contas locais”.

4. Neste diálogo, selecione “Clássico – os usuários locais são autenticados como eles próprios” e clique em “OK” para salvar.

Isto fará com que os usuários locais do domínio sejam autenticados como eles mesmos, mesmo que não estejam no “local” do servidor em questão. Sem isso, todos os usuários remotos, mesmo os usuários localizados fisicamente no domínio, serão autenticados como “convidados” e, provavelmente, não terão credenciais suficientes para realizar uma auditoria remota.

Observe que a ferramenta **`gpedit.msc`** não está disponível em algumas versões, como Windows 7 Home, que não tem suporte da Tenable.

Configurar uma conta de domínio para varreduras autenticadas

Para criar uma conta de domínio para auditoria remota em host de um servidor Windows, o servidor deve ser um Windows Vista, Windows XP Pro, Windows 2003 ou Windows 2008 e fazer parte de um domínio. Há cinco etapas gerais que devem ser executadas para facilitar essa verificação ao passo que mantém a segurança.

Etapa 1: Criação de um grupo de segurança

Primeiro, crie um grupo de segurança chamado **Nessus Local Access** (Acesso local Nessus):

- Faça login em um controlador de domínio e abra usuários e computadores do diretório ativo.

- Crie um grupo de segurança no **Menu**, selecione **Action** (Ação) -> **New** (Novo) -> **Group** (Grupo).

- Nomeie o grupo como **Nessus Local Access** (Acesso local Nessus). Certifique-se de que ele tem um “Scope” (Escopo) `Global` e um “Type” (Tipo) `Security` (Segurança).

- Adicione a conta que será usada para realizar as varreduras autenticadas Nessus para Windows no grupo **Nessus Local Access** (Acesso local Nessus).

Etapa 2: Criar uma política de grupo
Em seguida, será necessário criar uma política de grupo chamada **Local Admin GPO** (GPO admin local).

- Abra o **Group Policy Management Console** (Console de gerenciamento de políticas de grupo).

- Clique com o botão direito em **Group Policy Objects** (Objetos da política de grupo) e selecione **New** (Novo).

- Digite o nome da política: **Nessus Scan GPO** (GPO de varredura Nessus).

Etapa 3: Configurar a política para adicionar o grupo “Nessus Local Access” (Acesso local Nessus) **como administradores**
Aqui, adicionaremos o grupo **Nessus Local Access** (Acesso local Nessus) à política **Nessus Scan GPO** (GPO de varredura Nessus) e os colocaremos nos grupos que desejamos usar.

- Clique com o botão direito na política “**Nessus Scan GPO**” (GPO de varredura Nessus) e, em seguida, selecione **Edit** (Editar).

- Expanda ***Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups*** (Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Grupos Restritos).

- No painel esquerdo em **Restricted Groups** (Grupos restritos), clique com o botão direito e selecione “**Add Group**” (Adicionar grupo).

- Na caixa de diálogo “**Add Group”** (Adicionar grupo), selecione Procurar e digite **Nessus Local Access** (Acesso local Nessus) e, em seguida, clique em “**Check Names”** (Verificar Nomes).

- Clique em **OK** duas vezes para fechar a caixa de diálogo.

- Clique em **“Add”** (Adicionar) em “***This group is a member of:***” *(Este grupo é um membro de:)*

- Adicione o grupo “*Administrators” (Administradores)*.

- Clique em **OK** duas vezes.

Etapa 4: Certifique-se de que as portas corretas estão abertas no firewall para que o Nessus se conecte ao host
O Nessus usa SMB (bloqueio de mensagens do servidor) e WMI (Instrumentação de Gerenciamento do Windows) para isso, precisamos nos certificar de que o Firewall do Windows permitirá o acesso ao sistema.

Permissão do WMI no Firewall do Windows XP e 2003

- Clique com o botão direito na política “**Nessus Scan GPO**” (GPO de varredura Nessus) e selecione “**Edit**” (Editar).

- Expanda ***Computer configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile*** (Configuração do Computador\Políticas\Modelos Administrativos\Rede\Conexões de Rede\Firewall do Windows\Perfil de Domínio ou Perfil Padrão).

    - ***Observação***: O motivo principal do Perfil do domínio ser configurado, e não o perfil padrão, é que o Perfil de domínio será aplicado somente quando o Windows determinar que ele está conectado a uma rede que é parte do domínio do qual o perfil é membro. O perfil padrão será aplicado quando os hosts não puderem determinar se ele está em uma rede que faz parte do domínio ou em uma rede pública, então, minimizando a exposição às portas de WMI reduzirá o risco.

- Selecione “**Windows Firewall: Define inbound program exceptions**” (Firewall do Windows: definir exceções de programas de entrada) e clique com o botão direito e selecione “**Edit**” (Editar) (ou clique duas vezes nele com o mouse).

  - Selecione “**Enabled**” (Habilitado)

  - Clique em “**Show**” (Mostrar)

  - Nas definições de “**Program Exceptions**” (Exceções de programa) insira:

    - %windir%\system32\wbem\unsecapp.exe:*:enable:wmi

    - %windir%\system32\dllhost.exe:*:enable:ddlhost

    - ***Observação***: nas entradas acima, o * atua como um caractere curinga para permitir que qualquer endereço IP no domínio se conecte a esses serviços. Será possível tornar isso mais seguro permitindo endereços IP e intervalos onde as ferramentas administrativas se conectarão à porta ou onde for o endereço IP do scanner Nessus.

  - Clique em **OK**

  - Clique em **OK** para ir até a lista de políticas do firewall.

- Selecione “**Windows Firewall: Allow local port exceptions**” (Firewall do Windows: permitir exceções de portas locais) e clique com o botão direito e selecione **“Edit”** (Editar) (ou clique duas vezes nele com o mouse).

  - Selecione “**Enabled**” (Habilitado)

  - Clique em **OK**

- Selecione “**Windows Firewall: Define inbound port exceptions”** (Firewall do Windows: definir exceções de portas de entrada) e clique com o botão direito e selecione “**Edit”** (Editar) (ou clique duas vezes nele com o mouse).

  - Selecione **“Enabled**” (Habilitado)

  - Clique em **“Show**” (Mostrar)

  - Nas definições de **“Port Exceptions**” (Exceções de porta) insira:

    - 135:TCP:*:enable

    - ***Observação***: nas entradas acima, o * atua como um caractere curinga para permitir que qualquer endereço IP no domínio se conecte a esses serviços. Será possível tornar isso mais seguro permitindo endereços IP e intervalos onde as ferramentas administrativas se conectarão à porta ou onde for o endereço IP do scanner Nessus.

  - Clique em **OK** para ir até a lista de políticas do firewall.

- Selecione “**Windows Firewall: Define inbound program exceptions**” (Firewall do Windows: definir exceções de programas de entrada) e clique com o botão direito e selecione “Editar” (Editar) (ou clique duas vezes nele com o mouse).

  - Selecione **“Enabled**” (Habilitado)

  - Clique na caixa de “**Allow unsolicited incoming messages from these IP adresses**” (Permitir mensagens de entrada não solicitadas desses endereços IP) e digite *

- ***Observação***: nas entradas acima, o * atua como um caractere curinga para permitir que qualquer endereço IP no domínio se conecte a esses serviços. Será possível tornar isso mais seguro permitindo endereços IP e intervalos onde as ferramentas administrativas se conectarão à porta ou onde for o endereço IP do scanner Nessus.

- Clique em **OK** para ir até a lista de políticas do firewall.

Permissão do WMI no Firewall do Windows Vista, 7, 8, 2008, 2008R2 e 2012

- Clique com o botão direito na política "**Nessus Scan GPO**" (GPO de varredura Nessus) e selecione "**Edit**" (Editar).

- Expanda ***Computer configuration\Policies\Windows Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules*** (Configurações do Computador\Políticas, Configurações do Windows\Configurações de Segurança\Firewall do Windows com Segurança Avançada\Regras de Entrada)

- Clique com o botão direito na área de trabalho e selecione **New Rule...** (Nova regra...)

- Selecione a opção predefinida e selecione **Windows Management Instrumentation (WMI) (Instrumentação de Gerenciamento do Windows (WMI))** na lista suspensa.

- Clique em **Next** (Avançar)

- Marque as caixas de seleção de:

  - Windows Management Instrumentation (Instrumentação de Gerenciamento do Windows (ASync-In))

  - Windows Management Instrumentation (Instrumentação de Gerenciamento do Windows (WMI-In))

  - Windows Management Instrumentation (Instrumentação de Gerenciamento do Windows (DCOM-In))

- Clique em **Next** (Avançar)

- Clique em **Finish** (Concluir)

- ***Observação***: será possível editar posteriormente a regra predefinida criada e limitar a conexão às portas por meio de endereço IP e usuário do domínio, reduzindo, assim, qualquer risco de abuso da WMI.

Etapa 5: Vinculação de GPO

- O console de gerenciamento de políticas de grupo, clique com o botão direito no domínio ou em OU e selecione Link an Existing GPO (Vincular GPO existente)

- Selecione Nessus Scan GPO (GPO de varredura Nessus)

Configuração do Windows XP e 2003

Ao executar varreduras autenticadas de sistemas Windows XP ou 2003, várias opções de configuração devem ser ativadas:

1. O serviço WMI deve estar ativado no destino.

2. O serviço Registro remoto deve estar ativado (normalmente é desativado). Ele pode ser ativado manualmente para auditorias continuadas pelo administrador ou pelo Nessus. Usando os plugins 42897 e 42898, o Nessus pode ativar o serviço somente durante a varredura.

3. O compartilhamento de arquivos e impressoras deve estar ativado na configuração de rede de destino.

4. As portas 139 e 445 devem estar abertas entre o scanner Nessus e o destino.

5. Uma conta SMB com direitos locais de administrador no destino deve ser usada.

Não é necessário alterar as políticas locais de segurança do Windows, pois podem bloquear o acesso ou as permissões inerentes. Uma política comum que afetará as varreduras credenciadas pode ser encontrada em:

Ferramentas Administrativas -> Política de Segurança Local -> Configurações de Segurança -> Políticas locais -> Opções de segurança -> Acesso à rede: modelo de compartilhamento e segurança para contas locais.

Se esta política de segurança local estiver definida com uma opção diferente de “Clássico – os usuários locais são autenticados como eles próprios”, a varredura de conformidade não será executada.

Configuração do Windows 2008, Windows Vista e Windows 7

Ao executar varreduras autenticadas de sistemas Windows 2008, Windows Vista ou Windows 7, várias opções de configuração devem ser ativadas:

1. Em Firewall do Windows -> Configurações do Firewall do Windows, “Compartilhamento de Arquivos e Impressoras” deve estar selecionado.

2. Com a ferramenta **`gpedit.msc`** (no prompt “Executar...”, acesse o Editor de Objeto de Diretiva de Grupo. Navegue até Diretiva de Computador Local -> Modelos Administrativos -> Rede -> Conexões de Rede - > Firewall do Windows -> Perfil Padrão -> Firewall do Windows: permitir exceção no compartilhamento de impressoras e arquivos e habilitá-la.

3. No Editor de Objetos de Diretiva de Grupo, Diretiva de Computador Local -> Modelos Administrativos -> Rede -> Conexões de Rede -> Proibir uso do Firewall de conexão com a Internet na rede do domínio DNS deve estar definido como “Desativado” ou “Não Configurado”.

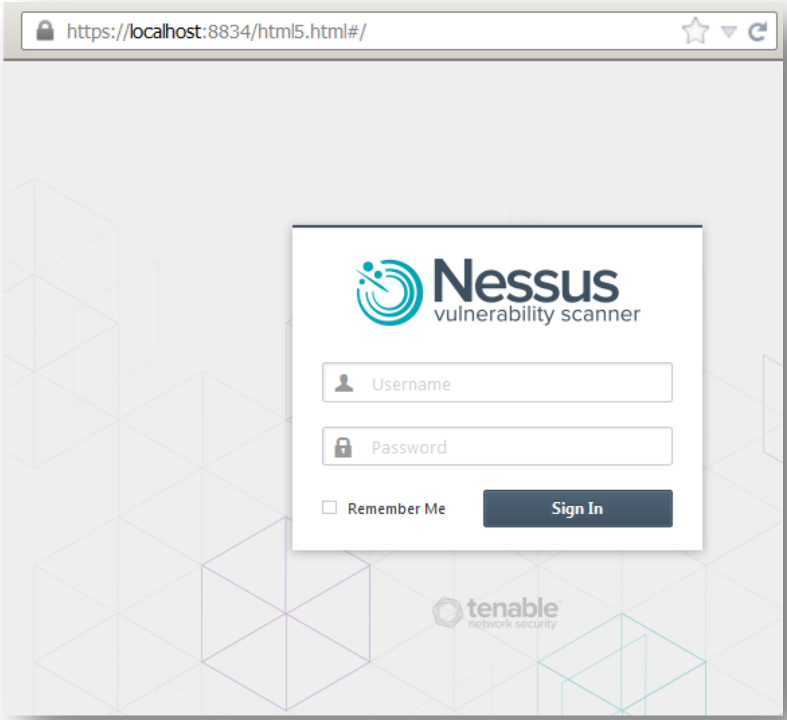
4. O serviço Registro remoto deve estar ativado (normalmente é desativado). Ele pode ser ativado manualmente para auditorias continuadas pelo administrador ou pelo Nessus. Usando os plugins 42897 e 42898, o Nessus pode ativar o serviço somente durante a varredura.

> O Nessus tem a capacidade de ativar e desativar o serviço Registro remoto. Para que isso funcione, o destino deve ter o serviço Registro remoto definido como “Manual” e não “Desabilitado”.

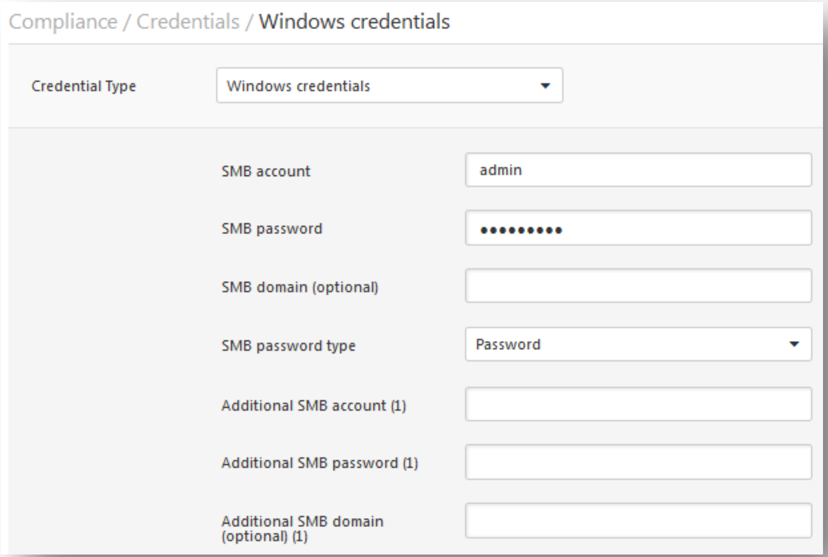
> Como alternativa, o Controle de conta do usuário (UAC) do Windows pode ser desativado, mas esta ação não é recomendada. Para desativar completamente o controle de contas, abra o Painel de Controle, selecione “Contas de Usuário” e “Desativar Controle de Conta do Usuário”. Também é possível criar uma nova chave de registro chamada “LocalAccountTokenFilterPolicy” e atribuir a ela o valor “1”. Essa chave deve ser criada no registro no seguinte local: **`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`**. Para obter mais informações sobre configurações de registro, consulte MSDN 766945 KB.

Configurar o Nessus para login do Windows

Interface de usuário do Nessus



Abra um navegador e conecte-se à interface de usuário do scanner Nessus como no exemplo acima e clique na guia "Policies" (Políticas). Crie uma nova política ou edite uma política existente e selecione a guia "Credentials" (Credenciais) à esquerda. Selecione “Windows credentials” (Credenciais do Windows) no menu suspenso na parte superior, conforme mostrado abaixo:



Especifique o nome da conta do SMB, a senha e o domínio opcional.

Neste ponto, clique em “**Submit**” (Enviar) na parte inferior da janela para concluir a configuração. A nova política de varredura será adicionada à lista de políticas de varredura gerenciadas.

Linha de comando do Nessus para Unix

Uso dos arquivos .nessus

O Nessus pode salvar políticas de varredura configuradas, alvos de rede e relatórios como arquivo **`.nessus`**. A seção acima “Interface de Usuário do Nessus” descreve a criação de um arquivo **`.nessus`** que contém credenciais do Windows. Para obter instruções sobre como executar uma varredura por linha de comando com o arquivo **`.nessus`**, consulte o “Nessus User Guide” (Guia do usuário do Nessus) disponível em:

http://www.tenable.com/products/nessus/documentation

Uso dos arquivos .nessusrc

Se o arquivo “**`.nessusrc`**” for criado manualmente, existem três itens que permitem a configuração do nome do usuário, senha e domínio opcional, conforme indicado abaixo:

```
Login configurations[entry]:SMB account : =
Login configurations[password]:SMB password : =
Login configurations[entry]:SMB domain (optional) : =
```

Detecção de falha de credenciais

Se o Nessus for usado para realizar auditorias credenciadas em sistemas Unix ou Windows, pode ser difícil analisar os resultados para saber o usuário tem as senhas e chaves SSH corretas. Com a nova versão do Nessus, os usuários podem detectar facilmente se suas credenciais estão funcionando. A Tenable incluiu o plugin Nessus #21745 na família de plugins “Settings”.

Este plugin detecta se as credenciais do SSH ou do Windows permitiram o acesso da varredura ao host remoto. Se o login for realizado com sucesso, o plugin não irá gerar nenhum resultado. Veja a seguir um exemplo de relatório gerado após a tentativa de login em um computador remoto com o nome de usuário ou a senha incorreta por meio do Nessus:



Solução de problemas

P. Como saber se a varredura local está funcionando?

R. A menos que o servidor esteja 100% atualizado, qualquer varredura local provavelmente gerará algum tipo de informação sobre patches. Dependendo do sistema operacional, ele também gerará várias informações de auditoria.

Também pode ser útil retirar o “Nessus” da equação e testar para garantir que as contas e as redes estão configuradas corretamente. No scanner Nessus, use o comando **id** simples do Unix e execute o seguinte comando:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
#
```

Verifique se está usando o endereço IP do sistema com o qual a relação de confiança está configurada, bem como a conta de usuário (neste caso, o usuário “nessus”). Se o comando for executado corretamente, você verá os resultados do comando **id** como se fosse executado no seu sistema remoto.

Nas auditorias do Unix, o script **ssh_get_info.nasl** indicará se a autenticação foi bem-sucedida. Se os logins com o SSH não estiverem funcionando, altere a configuração de “report_verbosity” da varredura do Nessus para “Verbose”. Isto exibirá todos os erros ou as mensagens de diagnóstico enquanto este script específico estiver em execução.

Nas auditorias do Windows, os scripts **smb_login.nasl** e **smb_registry_access.nasl** indicam se o login e a senha fornecidos durante a varredura funcionaram e se fosse possível ler o registro remoto. O **smb_registry_full_access.nasl** avisa apenas se não foi possível ler completamente o registro. O exame dos resultados das verificações de host em auditorias de um servidor Windows mostrará como as credenciais funcionaram.

Além disso, o script **hostlevel_check_failed.nasl** detecta se as credenciais do SSH ou do Windows não permitiram o login da varredura no host remoto.

P. Como saber se a varredura local não está funcionando?

R. Em sistemas Windows, as ocorrências de falha de logon são geradas no servidor. Se um controlador de domínio estiver em uso, as ocorrências de falha de login também estarão localizadas aí.

Em sistemas Unix, as falhas de login aparecerão nos logs de sistemas (como **`/var/log/messages`**), a menos que seja usado um controlador Kerberos remoto.

Além disso, o script **`hostlevel_check_failed.nasl`** detecta se as credenciais do SSH ou do Windows não permitiram o login da varredura no host remoto.

P. Quais outros eventos podem afetar as verificações do host?

R. Muitas situações podem bloquear o acesso. Algumas delas são:

- Firewalls de rede que filtram a porta 22 para SSH no Unix, ou a porta 445 no Windows.
- Firewalls de host que bloqueiam conexões com as portas mencionadas.
- Em sistemas Unix, os administradores podem alterar o SSH para portas diferentes de 22.
- Alguns sistemas de prevenção de invasão de hosts e rede impedem o acesso remoto.
- O computador examinado não é um servidor Unix ou Windows, mas pode ser uma impressora, roteador, aparelho de fax ou dispositivo de vídeo.

P. Estou realizando testes de conexões SSH do prompt do shell de hosts de varredura de destino para o sistema Nessus para garantir a conectividade. No entanto, acho que existe um atraso na conexão. Por quê?

R. Isto provavelmente ocorre porque o sistema está executando uma pesquisa de DNS quando o DNS está configurado incorretamente. Se o site usar DNS, entre em contato com o administrador do DNS para resolver os problemas de configuração. Um desses problemas pode ser a falta de zonas de pesquisa inversa. Para testar as pesquisas de DNS, faça o seguinte:

```
# host IP_ADRR_OF_NESSUS_SERVER
```

Se tiver o “dig” instalado também é possível verificar com:

```
# dig -x IP_ADRR_OF_NESSUS_SERVER
```

Se o site não usar DNS, as seguintes etapas irão ignorar a tentativa de realizar pesquisas de DNS.

1. Edite o arquivo **`/etc/nsswitch.conf`** para que as linhas “hosts:” exibam “hosts: files”
   Obs.: Isto não deve funcionar com todas as versões do OpenSSH.
2. Adicione no arquivo **`/etc/hosts`** do sistema o IP/nome do servidor que executa o Nessus.
3. Configure o servidor OpenSSH remoto para **não** realizar pesquisas de DNS em um host configurando:
   - “UseDNS no” no arquivo **`sshd_config`** (na versão 3.8), o valor padrão é yes (sim).
   - “VerifyReverseMapping no”

Proteção do scanner

Por que devo proteger meu scanner?

Se o scanner Nessus for configurado para usar credenciais para fazer login em um servidor Unix ou Windows, seu sistema terá credenciais que podem ser usadas por um usuário mal-intencionado. Para prevenir isso, é preciso por em prática uma diretiva de segurança adequada no sistema operacional em que o scanner está instalado e estar ciente de como o invasor pode obter informações de segurança do scanner.

O que significa bloquear um scanner?

O scanner Nessus apropriado deve ser controlado inteiramente de um console do sistema e não aceitar nenhuma conexão de rede de nenhum host remoto. O sistema deve estar fisicamente protegido, de modo que apenas as pessoas autorizadas tenham acesso a ele. Além disso, o servidor deve estar protegido com um firewall externo ou switch que permite examinar apenas redes específicas. Não instale um software de firewall pessoal diretamente no sistema do scanner Nessus. Lembre-se que o Nessus pode ser configurado para examinar apenas redes específicas.

Esse tipo de scanner não é muito usado. É preciso liberar o acesso remoto da rede ao servidor. O Nessus oferece suporte para conexões HTTP com a porta 8834. O firewall do sistema pode ser configurado para aceitar apenas conexões na porta 8834 de clientes Nessus válidos.

Se o dispositivo for administrado ou controlado de maneira remota, o acesso remoto seguro também pode ser usado. No Unix, o protocolo Secure Shell (SSH) pode ser usado. Mantenha o daemon do SSH atualizado, use senhas e/ou técnicas de autenticação otimizadas. Nos servidores Windows, os serviços de terminal remoto podem ser usados para fornecer comando e controle sobre os serviços para o Nessus Windows. Em ambos os casos, mantenha o sistema atualizado e não execute serviços de rede desnecessários. Consulte os benchmarks CIS (Center for Internet Security) (referenciais do CIS (Center for Internet Security)) para obter orientações sobre como reforçar os sistemas.

Implementação segura de auditorias de SSH no Unix

Nunca use senhas de SSH para executar varreduras remotas. Se uma rede for examinada, um invasor ou usuário mal-intencionado precisaria executar apenas um daemon de SSH para modificar e alterar o nome de usuário e a senha. Mesmo que esteja usando uma combinação diferente de nome de usuário e senha em cada máquina, o uso de senhas estáticas continua sendo vulnerável à exploração.

Caso o usuário efetue login em um servidor usando uma senha em um sistema que foi comprometido, haverá a chance da senha ser roubada, pois a própria senha é tunelada pela conexão SSH. Depois do servidor remoto ser dominado, o invasor poderá substituir o daemon de SSH por um próprio, o que registrará as senhas das conexões de entrada.

Auditorias seguras do Windows

Se a opção “Only use NTLMv2” (Usar apenas o NTLMv2) estiver desativada, teoricamente é possível induzir o Nessus a tentar fazer login em um servidor Windows com credenciais de domínio por meio da versão 1 do protocolo NTLM. Isto permite que o atacante remoto use um “hash” obtido com o Nessus. Este “hash” pode ser decodificado para revelar o nome de usuário ou a senha. Também pode ser usado para fazer login diretamente em outros servidores. Force o Nessus a usar o NTLMv2 ao ativar a opção “Only use NTLMv2” (Usar apenas NTLMv2) no momento da varredura. Isto impede que um servidor Windows hostil use o NTLM e receba um “hash”.

O NTLMv2 pode fazer uso do “SMB Signing”. Verifique se “SMB Signing” está ativado em todos os seus servidores Windows para evitar qualquer servidor que obtenha um “hash” de uma varredura do Nessus o reutilize. Além disso, não deixe de aplicar uma política que determine o uso de senhas fortes que não possam ser facilmente decodificadas por meio de ataques de dicionário com ferramentas como John the Ripper e L0phtCrack.

Observe que existem diferentes tipos de ataques contra a segurança do Windows para extrair “hashes” de computadores para reutilização no ataque a servidores. “SMB Signing” acrescenta uma camada de segurança para impedir esses ataques de intermediários.

Para obter mais informações

A Tenable produziu uma variedade documentos que detalham a instalação, implementação e configuração, operação do usuário e testes gerais do Nessus:

- **Nessus 5.2 Installation and Configuration Guide (Guia de instalação e configuração do Nessus 5.2)** – instruções passo a passo da instalação e da configuração.
- **Nessus User Guide (Guia do Usuário Nessus 5.2)** – como configurar e operar a interface do usuário Nessus.
- **Nessus Compliance Checks (Verificações de Conformidade do Nessus)** – guia geral para compreender e executar verificações de conformidade com o Nessus e o SecurityCenter.
- **Nessus Compliance Checks Reference (Referência de Verificações de Conformidade do Nessus)** – guia completo da sintaxe das verificações de conformidade do Nessus.
- **Nessus v2 File Format (Formato de arquivo Nessus v2)** – descreve a estrutura do formato de arquivo **`.nessus`**, que foi introduzido com o Nessus 3.2 e NessusClient 3.2.
- **Nessus 5.0 REST Protocol Specification (Especificação do protocolo REST do Nessus 5.0)** – descreve o protocolo e a interface REST do Nessus.
- **Nessus 5 and Antivirus (Nessus 5 e antivírus)** – destaca como vários pacotes de softwares de segurança populares interagem com o Nessus, além de fornecer dicas e soluções para permitir que o software coexista melhor sem comprometer a segurança ou dificultar as ações de varredura de vulnerabilidades
- **Nessus 5 and Mobile Device Scanning (Nessus 5 e varredura de dispositivos móveis)** – descreve como o Nessus integra-se ao Microsoft Active Directory e aos servidores de gerenciamento de dispositivos móveis para identificar dispositivos móveis em uso na rede
- **Nessus 5.0 and Scanning Virtual Machines (Nessus 5.0 e a varredura de máquinas virtuais)** – descreve como o scanner Nessus de vulnerabilidades da Tenable Network Security pode ser usado para auditoria da configuração de plataformas virtuais, assim como os softwares em execução nelas
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE (Monitoramento estratégico antimalware com Nessus, PVS e LCE)** – descreve como a plataforma USM da Tenable pode detectar uma variedade de softwares maliciosos, além de identificar e determinar a extensão das contaminações por malwares
- **Patch Management Integration (Integração com gerenciamento de patches)** – o documento descreve como o Nessus e o SecurityCenter podem explorar as credenciais nos sistemas de gerenciamento de patches IBM TEM, Microsoft WSUS e SCCM, VMware Go e Red Hat Network Satellite para realizar a auditoria de patches nos sistemas dos quais as credenciais podem não estar disponíveis ao scanner Nessus
- **Real-Time Compliance Monitoring (Monitoramento de Conformidade em Tempo Real)** – descreve como as soluções da Tenable podem ser usadas para ajuda a cumprir muitos tipos diferentes de normas do governo e do setor financeiro.
- **Tenable Products Plugin Families (Famílias de plugins dos produtos Tenable)** – fornece a descrição e o resumo das famílias de plugins para Nessus, Log Correlation Engine e Passive Vulnerability Scanner
- **SecurityCenter Administration Guide (Guia de administração SecurityCenter)**

Outros recursos on-line são listados a seguir:

- Nessus Discussions Forum (Fórum de Discussão do Nessus): https://discussions.nessus.org/
- Tenable Blog (Blog da Tenable): http://www.tenable.com/blog

- Tenable Podcast (Podcast da Tenable): http://www.tenable.com/podcast
- Example Use Videos (Vídeo de exemplos de uso): http://www.youtube.com/user/tenablesecurity
- Tenable Twitter Feed (Feed do twitter da Tenable): http://twitter.com/tenablesecurity

Entre em contato conosco pelo e-mail support@tenable.com, sales@tenable.com ou visite nosso site no endereço http://www.tenable.com/.

Sobre a Tenable Network Security

A Tenable Network Security conta com a confiança de mais de 20 mil empresas, incluindo todo o Departamento de Defesa dos EUA, além de diversas das maiores empresas do mundo e governos, para manter-se à frente das vulnerabilidades, ameaças e riscos de conformidade emergentes. Suas soluções, Nessus e SecurityCenter, continuam a definir o padrão para identificar vulnerabilidades, evitar ataques e estar em conformidade com uma ampla variedade de requisitos normativos. Para mais informações, visite www.tenable.com.

SEDE GLOBAL

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

tenable™ network security

Copyright © 2014. Tenable Network Security, Inc. Todos os direitos reservados. Tenable Network Security e Nessus são marcas comerciais registradas da Tenable Network Security, Inc.